REMARKS

Claims 1-18 are pending in this application. Applicants thank the Examiner for withdrawing the various objections and the rejections under 35 U.S.C. §§ 101 and 112, first paragraph.

Rejections Under 35 U.S.C. § 103

Claims 1-6 and 8-18 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Futa U.S. Patent No. 7,130,422 and Hopkins U.S. Patent Pub. No. 2005/0190912 A1. Claim 7 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Futa, Hopkins and Matyas U.S. Patent No. 4,736,423. Applicants respectfully traverse these rejections.

As discussed in more detail in the previous response, Applicants' claims are directed to a method of generating electronic keys for a public-key cryptography method using an electronic device. The claims also relate to a secure portable object using the claimed method.

Applicants' claimed embodiments encompass the generation of keys for an RSA-type cryptography system and to their storage on a secure object that can be used, for example, in an application requiring security. The claimed subject matter can apply to secure objects that do not have a large memory resource, such as an electrically programmable memory, or powerful calculation resources, as is the case for chip cards. An embodiment can include, for example, electronic commerce implemented using a mobile telephone. In this context, the keys may be on the SIM card of the telephone, for example.

The claimed embodiments address a problem of calculation complexity associated with managing the generation of keys and also the problem of the lack of

flexibility due to the initial and definitive storage of a large number of keys and certificates during a personalization phase.

An embodiment relates to a method of generating electronic keys, d, for a public-key cryptography method using, for example, an electronic device, mainly characterized in that it comprises two separate calculation steps:

Step A, which includes 1) calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers. This calculation is independent of knowledge of the pair (e, l) in which e is the public exponent and l is the length of the key of the cryptography method, and where l is the length of the modulus N of the method, and 2) storing the pairs or values thus obtained; and Step B, which includes calculating the key, d, from the results of step A and knowledge of the pair (e, l).

Thus, the claimed embodiments provide a method that involves two separate steps, in which the second step - which can be performed very quickly compared to known solutions - can be carried out in real time. This embodiment can also use a relatively small amount of memory space.

Applicants respectfully submit that the same combination of elements is neither disclosed nor suggested by Futa, Hopkins or Matyas, viewed alone or in combination. For example, various sections of Futa (col. 9, lines 3-4 and lines 41-43 and col. 11, lines 6-10 and 13-14) are cited for support of the claimed method where pairs of prime numbers (p, q), or values representative of pairs of prime numbers, are calculated and stored independent of knowledge of the pair of values (e, l), in which e is the public exponent and l is the length of the key of the cryptography method. The Action, on page 3, states that "since the public key is calculated after

the prime numbers have been calculated, the generation of the prime numbers is not made with knowledge of the public key (i.e. e, l)." Applicants respectfully disagree.

The cited sections of Futa disclose a prime generating unit that uses a random number to generate two prime numbers, that the generated prime number p has a bit size twice the bit size of prime q, that a public key generating unit reads primes p_a and p_b and multiples them together to find integer $n = p_a \times p_b$ and that a public key generating unit receives random number e from the random number generating unit and calculates number $d = e^{-1} \bmod L$. According to Futa, the pair of integers n and e is the public key, whereas the pair of integers n and d is the secret key.

Futa also discloses, however, at col. 6, lines 41-56, that the generating unit may include a random number generating unit for generating a random number R' whose bit length is (Lenq - LenL-1), where Lenq is the bit length of the prime q and LenL is a bit length of $(L_1 \times L_2 \times \ldots . \times L_n)$; and a judgment target generating unit for (a) generating a number R where $R = L_1 \times L_2 \times \ldots . \times L_n \times R'$ using the random number R' and the primes $L_1, L_2, \ldots, L_n$, and (b) generating the number N where $N = 2 \times R \times q+1$ using the prime q and the number R, wherein the judging unit judges the primality of the number N, using the number N and the number R generated by the judgment target generating unit.

Thus, since Futa discloses that the length of the prime number q, which is half the length of p, and which when multiplied together create integer n, which is the key length, the above-cited sections of Futa do indeed disclose that the generation of the prime numbers is made with knowledge of the key, since the key length is set from the beginning of Futa's process. Thus, Futa's process is not independent of

knowledge of the pair of values (e, l), in which e is the public exponent and l is the length of the key.

Hopkins, which is cited only for allegedly providing a communications means, does not cure the deficiencies of Futa. Moreover, Hopkins, in the cited sections, merely discloses that a recipient may publish his or her public key. Thus, Applicants respectfully submit that the cited sections of Hopkins do not adequately teach or suggest the claimed communication means for receiving at least one pair of values (e, l).

Accordingly, independent claims 1 and 12 are allowable over the cited references. This logic also disposes of the rejections of claims 2-11 and 13-18, which depend directly or indirectly from claims 1 and 12 and add further distinguishing features. Claim 7 is also separately allowable because Futa and Hopkins are cited for teachings they do not provide and Matyas does not compensate for these deficiencies.

Conclusion

For the foregoing reasons, Applicants respectfully submit that this application is in immediate condition for allowance and all pending claims are patentably distinct from the cited references. Reconsideration and allowance of all pending claims are respectfully requested.

In the event that there are any questions about this application, the Examiner is requested to telephone Applicants' undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date April 24, 2009

By: /Brian N. Fletcher/
Brian N. Fletcher
Registration No. 51683

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

Customer No. 21839